Information Assurance Technology Analysis Center

Information Assurance Tools Report

Spring 98

VULNERABILITY ANALYSIS

8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838

703.902.3177

Fax 703.902.3425

STU-III 703.902.5869

STU-III Fax 703.902.3991

E-mail iatac@dtic.mil

http://www.iatac.dtic.mil

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Spring 1998	Spring 1998

4. TITLE AND SUBTITLE
Information Assurance Technology Analysis Center
Information Assurance Tools Report
Vulnerability Analysis

5. FUNDING NUMBERS
SPO700-97-R-0603

6. AUTHOR(S)
IATAC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC/AI
8725 John J. Kingman Road, #0944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This report provides an index of vulnerability analysis tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, providing users with a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool. As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database.

14. SUBJECT TERMS

Vulnerability Analysis

15. NUMBER OF PAGES
42

16. PRICE CODE None

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	U

TABLE OF CONTENTS

INTRODUCTION

The Information Assurance Technology Analysis Center (IATAC) is a Department of Defense (DoD) sponsored Information Analysis Center (IAC) that provides a central point of access for scientific and technical information (STINFO) regarding information assurance (IA) technologies, system vulnerabilities, research and development, and models and analyses. The overarching goal of the IAC is to aid in developing and implementing effective defenses against information warfare attacks. IATAC basic services include support for user inquiries, analysis, maintenance, and growth of the IA library; IA database operations; development of technical and state-of-the-art reports; and promotional awareness activities, such as newsletters, conferences, and symposia.

IACs are staffed by scientists, engineers, and information specialists. Each IAC establishes and maintains comprehensive knowledge bases that include historical, technical, scientific, and other data and information collected worldwide. Information collections span a wide range of unclassified, limited distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques including databases, models, and simulations. Their collections and products represent intensive evaluation and screening efforts to create authoritative sources of evaluated data.

This report addresses the contents of the Information Assurance Tools Database, one of the knowledge bases maintained by IATAC. This database hosts information on intrusion detection, vulnerability analysis, firewalls, and antivirus software applications. Information for this database is obtained via open-source methods, including direct interface with various agencies, organizations, and vendors.

PURPOSE

This report provides an index of vulnerability analysis tool descriptions contained in the IATAC Information Assurance Tools Database. This report summarizes pertinent information, providing users with a brief description of available tools and contact information. It does not endorse or evaluate the effectiveness of each tool.

As a living document, this report will be updated periodically as additional information is entered into the Information Assurance Tools Database. Technical questions concerning this report may be addressed to James Green at (703) 902-4887 or iatac@dtic.mil.

SCOPE

Currently the IATAC database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment. Vulnerability analysis tools are programs that help automate the identification of vulnerabilities in a network or system. Vulnerabilities can be defined as weaknesses in a systems security scheme exploitation of which would negatively affect the confidentiality, integrity, or availability of the system or its data. The type and level of detail of information provided among tools varies greatly. Although some can identify only a minimal set of vulnerabilities, others can perform a greater degree of analysis and provide detailed recommended countermeasures. More recently developed tools provide user-friendly front ends and sophisticated reporting capabilities. The majority of the tools identified in the Information Assurance Tools Database are available on the Internet, and many are used by crackers in the first stage of an attack: vulnerability information gathering. Penetration tools, which perform destructive actions (i.e., denial of service attacks), are excluded from this category. Sniffers, and Trojan horse programs are also excluded from this category. Although many network utilities (i.e., host, finger) are valuable in identifying vulnerabilities on a host, they are often an automated component of vulnerability analysis tools, and therefore are not individually described in the database.

The database includes commercial products, individual-developed tools, government-owned tools, and research tools. The database was built by gathering as much open-source data, analyzing that data, and summarizing information regarding the basic description, requirements, availability and contact information for each vulnerability analysis tool collected. Generally, the commercially developed products are available. The government and academic tools, however, are reserved for specific projects and organizations. The research group or university determines, on an individual case basis, the availability of these research tools. These tools are included in the database solely to provide infor-

mation regarding existing approaches for vulnerability analysis.

DATABASE FORMULATION

This section discusses the approach and methodology used for identifying and collecting the selected tools, the classification of each type, tool sources, and the structure of the database.

TOOL COLLECTION

Information for each tool was collected by leveraging existing community relationships. Collection activities included Internet searches to identify additional corporations, government agencies, professional organizations, and universities with involvement in vulnerability analysis. Industry professionals were consulted for information and suggestions for identifying and collecting available tools.

TOOL CLASSIFICATION

The vulnerability analysis tools described in the IATAC Information Assurance Tools Database fall within one or more of the following five classes:

Simple Vulnerability Identification and Analysis A number of tools have been developed that perform relatively limited security checks. These tools may automate the process of scanning Transmission Control Protocol/Internet Protocol (TCP/IP) ports on target hosts, attempting to connect to ports running services with well-known vulnerabilities and recording the response. They also may perform secure configuration checks for specific system features (e.g., network file system [NFS] configuration, discretionary access control [DAC] settings). The user interface of these tools is likely to be command-line based, and the reporting may include limited analysis and recommendations. These tools are also likely to be "freeware."

Comprehensive Vulnerability Identification and Analysis More sophisticated vulnerability analysis tools have been developed that are fairly comprehensive in terms of the scope of vulnerabilities addressed, the degree of analysis performed, and the extent of recommendations made to mitigate potential security risks. Many of these tools also provide a user-friendly graphical user interface.

War Dialers A war dialer consists of software that dials a specific range of telephone numbers looking for modems that provide a login prompt. The tools, at a minimum, record the modem numbers and login screen, but can also be configured to attempt brute force, dictionary-based, login attempts. The value of these tools to a system administrator is that they automate the process of identifying potential "back doors" in a network. Some of the tools described above in the "Comprehensive Vulnerability Identification and Analysis" category include war dialers.

Password Crackers Password cracker tools attempt to match encrypted forms of a dictionary list of possible passwords with encrypted passwords in a password file. This is possible because the algorithm used to encrypt operating systems' passwords is public knowledge. These tools support system administrators by allowing them to enforce password selection policies.

Risk Analysis Tools Risk analysis tools typically provide a framework for conducting a risk analysis but do not actually automate the vulnerability identification process. These tools may include large databases of potential threats and vulnerabilities along with a mechanism to determine, based on user input, cost-effective solutions to mitigate risks. The vulnerabilities identified using a true "vulnerability analysis" tool may be fed into a risk analysis tool.

TOOL SOURCES

Tools and information were identified from a number of sources. A representative sampling of these sources includes the following:

COMMERCIAL

AXENT Technologies, Inc.

Bellcore

Internet Security Systems

Intrusion Detection, Inc.

NETECT, Inc.

RiskWatch

Secure Networks Incorporated (SNI)

Somarsoft, Inc.

The Mitre Corporation

Trident Data Systems

WheelGroup Corporation*

* *On March 12, 1998, Cisco Systems completed its acquisition of WheelGroup Corporation.*

GOVERNMENT AND PROFESSIONAL AGENCIES AND RESEARCH CENTERS

ACM SIGSAC (Special Interest Group on Security, Audit, and Control)

Air Force Information Warfare Center

Defense Advanced Research Projects Agency (DARPA)

Center for Secure Information Systems (CSIS) at George Mason University

Central Intelligence Agency

COAST Project at Purdue University

Computer Security Research Laboratory at University of California at Davis

Computer Security Technology Center at Lawrence Livermore National Laboratory

Computing Professionals for Social Responsibility (CPSR)

Defense Information Systems Agency (DISA)

Department of Energy, Computer Incident Advisory Capability (CIAC)

IEEE-CS Technical Committee on Security and Privacy

IFIP Technical Committee 6 (Communication Systems)

IFIP Technical Committee 11 on Security and Protection in Information Processing

IFIP Working Group 11.3 on Database Security

IFIP Working Group 11.4 on Network Security

Information Sciences Institute, University of Southern California School of Engineering

Information Security Research Centre at Queensland University of Technology, Australia

Information Systems Audit and Control Research at CalPoly Pomona

Institute for Computer & Telecommunications Systems Policy at The George Washington University

International Association for Cryptologic Research

International Computer Security Association (ICSA)

Lawrence Berkeley National Laboratory

Los Alamos National Laboratory

National Institute of Standards and Technology (NIST) Computer Systems Laboratory

National Security Agency

Navy Research Laboratory Center for High Assurance Computer Systems (Naval Research Laboratory)

Navy Space and Naval Warfare Systems Command (SPAWAR)

SIRENE: SIcherheit in REchnerNEtzen (Security in Computer Networks) at the University of Hildesheim/IBM Zurich

Texas A&M University

U.S. Army Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4)

USENIX & System Administrators' Guild (SAGE)

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS)

Air Force Computer Emergency Response Team (AFCERT)

Army Computer Emergency Response Team (ACERT)

Australian Computer Emergency Response Team (AUSCERT)

CERT Coordination Center, Carnegie Mellon University

Computer Emergency Response Team for the German Research Network (DFN-CERT), German Federal Networks CERT, Germany

Computer Incident Advisory Capability (CIAC), U.S. Department of Energy

NASA Automated Systems Incident Response Capability (NASIRC)

Naval Computer Incident Response Team (NAVCIRT)

Purdue University Computer Emergency Response Team (PCERT)

SURFnet Computer Emergency Response Team (CERT-NL), Netherlands

Swiss Academic and Research Network CERT, Switzerland (SWITCH-CERT)

DATABASE STRUCTURE

The fields of the database include the following:

Title Name and abbreviation associated with the tool

Author Developer of the tool

Source Uniform resource locator (URL) of the primary source for obtaining the tool

Keyword Terms used to reference the tools using the database search engine

Contact Information Name, organization, telephone, facsimile, e-mail, and URL information for additional tool information

Abstract Brief description of the primary features of the tool

Requirements System requirements for operating the tool

Availability Accessibility information including procedures and pricing in some cases

TOOL SELECTION CRITERIA

The selected tools satisfy the following three criteria:

Definition These tools satisfy the objective, approach, and methodology of an vulnerability analysis tool based on the definition of vulnerability.

Specificity to Vulnerability Analysis The primary function of these tools is vulnerability analysis. They may also be used during the early stages of a penetration attack to identify the target system's weaknesses and help fine-tune the attack. However, penetration test tools, whose primary purpose is to exploit identified vulnerabilities and cause damage or destruction to the target system, have been excluded.

Current Availability These tools are currently available from the Government, academia, or commercial sources, or as freeware on the Internet.

RESULTS

The research for this report identified 35 vulnerability analysis tools currently being used and available. Appendix A includes complete database output for each tool. The content of Appendix A mirrors the database structure as defined in the "Database Structure" section of this report. The following summary chart provides the name, keywords, and a description of each tool.

Title	Source Type	Attributes	Contact / Organization	E-mail	URL
Ballista	Commercial	comprehensive vulnerability analysis	Secure Networks Inc.	sales@secnet.com	http://www.secnet.com/
CheckXusers	Individual	simple vulnerability analysis	Bob Vickers	R.Vickers@ulcc.ac.uk	http://www.ulcc.ac.uk/
Chkacct	Individual	simple vulnerability analysis	Shabbir Safdar	shabbir@panix.com	http://www.panix.com/~shabbir
CONNECT	Individual	simple vulnerability analysis	unknown	unknown	http://www.giga.or.at/pub/hacker/unix
COPS(Computer Oracle and Password System)	Individual	comprehensive vulnerability analysis	Dan Farmer	security@earthlink.net	http://www.earthlink.net/company/farmer.html
CPM (Check Promiscuous Mode)	Academia	simple vulnerability analysis	CERT Coordination Center	cert@cert.org	http://www.cert.org/contactinfo.html
Crack	Individual	password cracker	Alec Muffett	alec.muffet@uk.sun.com	http://www.users.dircon.co.uk/~crypto/index.html
Domain Obscenity Control(DOC)	Individual	simple vulnerability analysis	Steve Hotz	shotz@pollux.usc.edu	http://www.isi.edu/
DumpAcl	Commercial	simple vulnerability analysis	Somarsoft, Inc.	info@somarsoft.com	http://www.somarsoft.com/
Expert System for Progressive Risk Identification Techniques (ESPRIT)	Government	risk analysis	Rickey Roach	roachr@ncr.disa.mil	http://www.westhem.disa.mil/~WEY/esprit/
ICE-PICK	Government	comprehensive vulnerability analysis	Space and Naval Warfare Systems Center	questions@infosec.navy.mil	http://infosec.navy.mil/ICEPICK/
IdentTCPscan	Individual	simple vulnerability analysis	David Goldsmith	daveg@escape.com	http://www.giga.or.at/pub/hacker/unix
InternetScanner	Commercial	comprehensive vulnerability analysis	Patrick Taylor	info@iss.net	http://www.iss.net
Kane Security Analyst (KSA)	Commercial	misuse detection, system monitoring, comprehensive vulnerability analysis	Daniel Dorr	info@intrusion.com	http://www.intrusion.com/contact.htm
L0PHTCrack	Commercial	password cracker	L0PHT Heavy Industries	info@L0pht.com & admin@L0pht.com	http://www.L0pht.com/L0phtcrack/
Netective	Commercial	simple vulnerability analysis	NETECT Inc.	sales@netect.com	http://www.netect.com
NetRecon	Commercial	comprehensive vulnerability analysis	AXENT Technologies, Inc.	sundav@axent.com	http://www.axent.com/
NetSonar	Commercial	comprehensive vulnerability analysis	Joel McSarland	info@wheelgroup.com	http://www.wheelgroup.com/contact/1contact.html
Network Security Scanner(NSS)	Individual	comprehensive vulnerability analysis	Douglas O'Neal	Doug.ONeal@jhu.edu	http://www.jhu.edu/
Nfsbug	Individual	simple vulnerability analysis	Leendert van Doorn	leendert@cs.vu.nl	http://www.asmodeus.com/archive/Xnix/nfsbug/nfsbug.c
Omniguard/ESM	Commercial	comprehensive vulnerability analysis	AXENT Technologies, Inc	info@axent.com	http://www.axent.com/
Perl Cops	Individual	comprehensive vulnerability analysis	Dan Farmer	security@earthlink.net	http://www.earthlink.net/company/farmer.html
PINGWARE	Commercial	comprehensive vulnerability analysis	Bellcore	telecom-info@bellcore.com	http://telecom-info.bellcore.com/
RiskWatch v7.1	Commercial	risk analysis	Caroline R. Hamilton	riskwatch@riskguard.com	http://www.riskguard.com/prod01.htm
Security Analysis Tool for Auditing Networks(SATAN)	Individual	comprehensive vulnerability analysis	Dan Farmer	security@earthlink.net	http://www.earthlink.net/company/farmer.html
Secure Sun	Individual	simple vulnerability analysis	David Safford	d-safford@tamu.edu	http://www.cs.tamu.edu/
Snoopy Tools	Commercial	comprehensive vulnerability analysis	W. Reid Gerhart	wrg@mitre.org	http://www.mitre.org/resources/centers/infosec/infosec.html
SPI-NET	Government	comprehensive vulnerability analysis	Sandy Spark	ciac@llnl.gov	http://ciac.llnl.gov

Title	Source Type	Attributes	Contact Organization	E-mail	URL
Strobe	Individual	simple vulnerability analysis	Julian Assange	strobe@suburbia.net proff@suburbia.net	ftp://coast.cs.purdue.edu/pub /tools/unix/strobe/
System Security Scanner	Commercial	comprehensive vulnerability analysis	Patrick Taylor	info@iss.net	http://www.iss.net
Tiger	Academia	comprehensive vulnerability analysis	Doug Schales	Doug.Schales@net.tamu. edu	http://www.cs.tamu.edu/
ToneLoc	Individual	war dialers	Minor Threat and Mucho Maas	mthreat@paranoia.com - or-mthreat@ccwf.cc. utexas.edu	ftp://ftp.paranoia.com/pub/ toneloc/tl110.zip
Trident Information Protection Toolbox	Commercial	risk analysis	Brian Finan	Brian_Finan@tds.com	http://www.tds.com/tb/index. html#anal
Value of Information Structured Analysis of Risk Tool (VISART)	Government	risk analysis	Dr. Donald R. Peeples	n/a	http://www.nsa.gov/
Xscan	Individual	simple vulnerability analysis	unknown	pendleto@math.ukans. edu	http://www.giga.or.at/pub/ hacker/unix

TITLE

Ballista

AUTHOR

Secure Networks Inc.

SOURCE

http://www.secnet.com/nav1b.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Alfred Huger
Secure Networks Inc.
Suite 330, 1201 5th Street SW
Calgary, Alberta CANADA T2R-0Y6
Telephone: 403.262.9211
Facsimile: 403.262.9221
E-mail: sales@secnet.com
URL: http://www.secnet.com/

REQUIREMENTS

Solaris 2.5-2.6, Linux 2.x, BSDI 2.x, OpenBSD 2.x, FreeBSD 2.x, Windows NT 4.0

AVAILABILITY

Commercially available from http://www.secnet.com/. Evaluation copy available from http://www.secnet.com/nav1b.html. Licensing is based on a single host or specific addresses. Up to 10 addresses cost $150, up to 50 cost $350.

ABSTRACT

Ballista is a network security auditing tool used to discover security weaknesses in networked environments. Ballista uses extensive domain name system (DNS) auditing to map intranets and perform port scans. Vulnerability checks include file transfer protocol (FTP), Web Servers, Sendmail, RPC, NFS, NetBIOS, and network devices such as routers and bridges. Ballista also allows users to determine whether the filters of a firewall are securely configured and have password-guessing routines.

Secure Networks has developed a customizable tool included with Ballista, the Custom Auditing Packet Engine (CAPE). CAPE can perform complex protocol-level spoofing and attack simulations. CAPE also enables users to generate tool-sets onthefly to address unique network implementations. It can use custom scripts to verify the integrity of Access/Choke routers, filtering firewalls (statefull inspection or otherwise), etc. This modular architecture also allows Secure Networks to update Ballista easily and efficiently. Ballista's biweekly updates include new vulnerability checks and features.

TITLE

CheckXusers

AUTHOR

Bob Vickers

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Bob Vickers
University of London Computer Centre
20 Guilford Street
London ENGLAND WC1N 1DZ
Telephone: 0171.692.1000
Facsimile: 0171.692.1234
E-mail: R.Vickers@ulcc.ac.uk
URL: http://www.ulcc.ac.uk/

REQUIREMENTS

UNIX (Perl script); no special privileges; netstat command in PATH variable.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/checkXusers.Z

ABSTRACT:

CheckXusers identifies users logged onto the current machine from insecure X servers. It enables system administrators to determine whether users are exposing themselves, and hence the system, to unacceptable risks. It should be run from an ordinary user account, not root. It assumes that the netstat command is somewhere in the PATH prior to execution.

TITLE

Chkacct

AUTHOR

Shabbir Safdar

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/chkacct/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Shabbir Safdar
The Voters Telecommunications Watch
233 Court Street #2
Brooklyn, NY 11201
Telephone: 718.596.2851
Facsimile: n/a
E-mail: shabbir@panix.com
URL: http://www.panix.com/~shabbir

REQUIREMENTS

UNIX (Perl script); Audits account from which it is run.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/chkacct/chkacct.v1.1.tar.Z

ABSTRACT:

Chkacct was designed to complement tools like COPS and Tiger that check for configuration problems in an entire system. Chkacct is designed to check the settings and security of the current user's account. It identifies potential problems with the accountìs security and provides explanations of how to fix them. It may be preferable to have a security administrator ask problem users to run chkacct rather than directly alter files in their home directories.

Chkacct allows the user to check the security of his or her account quickly. It can be run out of a crontab in "harmless" mode and the output mailed to the user.

Chkacct checks the home directory for certain important "dot" files as well as searching throughout the entire home directory for files with all-user write permissions.

CONNECT

TITLE

CONNECT

AUTHOR

Unknown

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Name: Unavailable
Address: Unavailable
Telephone: Unavailable
Facsimile: Unavailable
E-mail: Unavailable
URL: Unavailable

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/connect.tar

ABSTRACT:

This /bin/sh shell script scans a range of Internet Protocol (IP) addresses for machines that offer the Trivial File Transfer Protocol (TFTP) service. Although typically disabled, this service is generally considered insecure and can be exploited to extract system files including /etc/passwd and other critical system files. If CONNECT finds a machine running TFTP, it will automatically attempt to download the /etc/passwd file to determine whether the system is vulnerable.

COPS

TITLE

Computer Oracle and Password System (COPS)

AUTHOR

Dan Farmer

SOURCE

ftp:// ftp.cert.org

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107
Telephone: 626.296.2400
Facsimile: 626.296.4130
E-mail: security@earthlink.net
URL: http://www.earthlink.net/company/farmer.html

REQUIREMENTS

UNIX (Perl script)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/cops/

ABSTRACT

Computer Oracle and Password System (COPS) is a security toolkit that examines a system for a number of known weaknesses and alerts the system administrator to them. In some cases it can automatically correct these problems. COPS identifies security vulnerabilities and checks for empty passwords in /etc/passwd, files with all-user write permissions, misconfigured anonymous ftp's, and many other area.

CPM

TITLE

Check Promiscuous Mode (CPM)

AUTHOR

CERT Coordination Center

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Telephone: 412.268.7090
Facsimile: 412.268.6989
E-mail: cert@cert.org
URL: http://www.cert.org/pub/aboutcert/contactinfo.html

REQUIREMENTS

UNIX (C source code), no special privileges

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/cpm/.

ABSTRACT

Check Promiscuous Mode (CPM) checks whether any network interface on a host is in promiscuous mode. A host in promiscuous mode can view all network traffic passing through its branch. CPM uses standard BSD UNIX socket (2) and ioct1(2) system calls to determine a system's configured network interfaces and reports whether any of the network interfaces are currently in promiscuous mode.

CPM identifies the number of interfaces found, the name of each interface, and whether each interface is in normal or promiscuous mode. It returns the number of discovered promiscuous interfaces as its exit status. No special privileges are required to invoke CPM.

TITLE

Crack

AUTHOR

Alec Muffett

SOURCE

ftp://ftp.cert.org/pub/tools/crack/

KEYWORD

password cracker

CONTACT INFORMATION

Alec Muffett
Sun Microsystems Ltd.
Sun House
306 Cambridge Science Park
Milton Road
Cambridge CB4 4WG
ENGLAND
Telephone: 01223.420421
Facsimile: 01223.420058
Email: alec.muffet@uk.sun.com
URL: http://www.users.dircon.co.uk/~crypto/index.html

REQUIREMENTS

UNIX (C source code, Perl script). Tested on Solaris, Linux, FreeBSD, NetBSD, OSF, and Ultrix. Root privileges to execute.

AVAILABILITY

Freely available from ftp://ftp.cert.org/pub/tools/crack/

ABSTRACT:

Crack is a password-cracking program with a configuration language that allows the user to program the types of guesses attempted. Crack is designed to quickly locate vulnerabilities in UNIX (or other) password files by scanning the contents of a password file and testing entries for weak (i.e., dictionary) passwords.

Crack helps the system administrator identify weak passwords by checking for various weaknesses and attempting to decrypt them. Systems employing shadowing password schemes are much harder to crack.

Crack's general procedure is to take as its input a series of password files and source dictionaries. It merges the dictionaries, turns the password files into a sorted list, and generates lists of possible passwords from the merged dictionary. Crack makes many individual passes over the password entries supplied as input. Each pass generates password guesses based on a sequence of rules.

Features include Eric Young's "libdes" encryption routines, an application programming interface (API) for ease of integration with arbitrary crypt() functions, API for ease of integration with arbitrary passwd file format, considerably better gecos-field checking, more powerful rule sets, ability to read dictionaries generated by external commands, better recovery mechanisms for jobs interrupted by crashes, improved control (e.g., disable during working hours). In addition, it comes bundled with Crack6 (minimalist password cracker) on with Crack7 (brute force password cracker).

DOC

TITLE

Domain Obscenity Control (DOC)

AUTHORS

Steve Hotz
Paul Mockapetris

SOURCE

http://csrc.nist.gov/tools/tools.htm

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Steve Hotz
Paul Mockapetris
University of Southern California School of Engineering Information Sciences Institute
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292-6695
Telephone: 310.822.1511
Facsimile: 310.823.6714
E-mail: shotz@pollux.usc.edu
URL: http://www.isi.edu/

REQUIREMENTS

UNIX (csh script)

Version 2.0 of the DNS query tool "dig" domain Internet groper

AVAILABILITY

Freely available at ftp://coast.cs.purdue.edu /pub/tools/unix/doc.2.0.tar.z

ABSTRACT:

Domain Obscenity Control (DOC) diagnoses misconfigured domains by sending queries to the appropriate domain name system (DNS) name servers and performing simple analysis on the responses. DOC verifies a domain's proper configuration and that it is functioning correctly. The domain name must be valid. Some changes to the script must be made including the first few aliases and pointers to directories.

DOC-V.2.0 is an initial implementation of an automated domain testing tool.

TITLE

DumpAcl

AUTHOR

Somarsoft, Inc.

SOURCE

http://www.somarsoft.com/

KEYWORD

simple vulnerability analysis

CONTACT INFORMATION

Somarsoft, Inc.
P.O. Box 642278
San Francisco, CA 94164-2278
Telephone: 415.776.7315
Facsimile: 415.776.7328
E-mail: info@somarsoft.com
URL: http://www.somarsoft.com/

REQUIREMENTS

Windows NT 3.51 or 4.0 (i386 and Alpha platforms). Targets Windows NT (any platform).

AVAILABILITY

Shareware version freely available from http://www.somarsoft.com/. Shareware version is fully functional except for printing. V2.7 adds enhancements and bug fixes for $99.

ABSTRACT:

Somarsoft DumpAcl dumps the permissions and audit settings for the Windows NT file system, registry, user/group information, and printers in a concise, readable, listbox format so the user can identify readily apparent security vulnerabilities.

Somarsoft DumpAcl provides a solution to the problem of having too many files and registry keys to manually check on a regular basis. Unnecessary system, file, and directory access can be identified from the tool's output.

ESPRIT

TITLE

Expert System for Progressive Risk Identification Techniques (ESPRIT)

AUTHOR

Joint Information Service Center of DISA

SOURCE

http://www.westhem.disa.mil/~WEY/esprit/

KEYWORD

risk analysis

CONTACT INFORMATION

Rickey Roach
Defense Information Systems Agency
Alexandria, VA 22204
Telephone: 703.607.4215
Facsimile: n/a
E-mail: roachr@ncr.disa.mil
esprit@ncr.disa.mil
URL: http://www.westhem.disa.mil/~WEY/esprit/

REQUIREMENTS

IBM-compatible PC 386, MS-DOS version 3.3 or higher, 13 MB of disk space, 2 MB RAM

AVAILABILITY

Available to approved Government agencies from http://www.westhem.disa.mil/~WEY/ esprit/

ABSTRACT

ESPRIT was developed for the Joint Staff Support Center (JSSC) in support of its continuing efforts to define and develop cost-effective procedures to assist in performing risk analysis. ESPRIT is a risk analysis and risk management tool to aid Department of Defense (DoD) risk analysts in performing automated information systems (AIS) risk analysis.

ESPRIT checks for risk-management compliance and is an automated tool to conduct certification. It provides a detailed analysis of an information system in terms of assets, threats to assets, vulnerabilites, and countermeasure recommendations. ESPRIT analysis indicates the current security level and gathers data needed to select adequate and cost-effective safeguards. It includes a database of pre-ranked vulnerabilities in order of their relative severity (i.e., high, medium, or low). The program posts the ranking of each vulnerability identified on the target system.

ESPRIT's database also contains countermeasure statements and descriptions. With predefined links between the vulnerabilities and the appropriate countermeasures. Answers to the initial questionnaires trigger an automatic linkup between an inferred vulnerability and its associated appropriate countermeasure.

A userid and password must be obtained (this can be done from the Web page) to download the program from the Web site.

ICE-PICK

TITLE

ICE-PICK

AUTHOR

SPAWAR

SOURCE

http://infosec.navy.mil/ICEPICK/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Commanding Officer
Code 72
Space and Naval Warfare Systems Center
Charleston SC (SPAWARSYSCEN)
P.O. Box 190022
North Charleston, SC 29419-9022
Telephone: 800.304.4636
Facsimile: n/a
E-mail: questions@infosec.navy.mil
URL: http://infosec.navy.mil/ICEPICK/

REQUIREMENTS

Version 1.2 - UNIX running Sunos 4.1.x, 4MB RAM; graphical interface such as Motif, Openwindows, or Xwindows; version 1.3 - Alpha Developments; portability to HP-UX version 10

AVAILABILITY

Available to approved Government agencies from ftp://infosec.navy.mil/pub/DOCs/navy /ice_req.DOC

ABSTRACT

ICE-PICK is U.S. Government property and is strictly controlled by SPAWAR for official Government use only. Unauthorized use, distribution, reproduction, or possession may be grounds for criminal prosecution including imprisonment. The complete ICE-PICK package is a security tool, for use by the system administrator tin identifying and fixing potential vulnerabilities.

ICE-PICK is an automated security tool used for evaluating the vulnerabilities of network-based systems that use TCP/IP. The tool is used to evaluate and rate the vulnerability of individual systems to various security threats that may be applied.

ICE-PICK is being distributed by the SPAWAR Systems Center Charleston SC to all Navy and Marine units. A Memorandum of Agreement must be signed by each requesting activity prior to release of the tool.

TITLE

IdentTCPscan

AUTHOR

David Goldsmith

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

David Goldsmith
Address: Unavailable
Telephone: Unavailable
Facsimile: Unavailable
E-mail: daveg@escape.com
URL: Unavailable

REQUIREMENTS

UNIX (C source code). Tested on BSDI, Linux 2.x, and SunOS 4.1.x.

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/identTCPscan.c.gz

ABSTRACT

IdentTCP scans remote hosts for active Transmission Control Protocol (TCP) services. In addition, the tool attempts to determine the UID of the running processes. Processes that execute as root will be targeted first by system crackers, because any manipulation of those services is more likely to give root access to the system. System administrators can use this utility to determine which services may be targeted and then evaluate the necessity of running the service as root. Output is comprehensive and easy to read.

INTERNET SCANNER

TITLE

Internet Scanner

AUTHOR

Internet Security Systems

SOURCE

http://www.iss.net/prod/isb.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East
Suite 660
Atlanta, GA 30346
Telephone: 770.395.0150
Facsimile: 770.395.1972
E-mail: info@iss.net
URL: http://www.iss.net

REQUIREMENTS

Windows NT 4.0, IBM AIX™ 3.25 and higher, HP-UX 9.05 and higher, Sun Solaris 2.3 and higher, Sun Solaris x86, SunOS 4.1.3 and higher, Linux 1.2x and 1.3x (with kernel patch), and Linux 1.3.7.6 and higher (no patch required). Disk space/memory requirements: Windows NT (10/24 MB); UNIX (5/24 MB).

AVAILABILITY

Commercial, single-host web scans cost approximately $1,500. Evaluation copy available from http://www.iss.net

ABSTRACT

The Internet Scanner tool set focuses on identifying and addressing network vulnerabilities. They perform scheduled and selective probes of network communication services, operating systems, key applications, and routers in search of common vulnerabilities that open the network to attack. Internet Scanner analyzes vulnerability conditions and provides sets of corrective action, trends analysis, conditional and configuration reports, and data sets.

Internet Scanner consists of three integrated modules for scanning intranets, scanning firewalls, and scanning Web servers. These modules are available singly, or as part of the Internet Scanner bundle.

Internet Scanner's intranet module is a network security assessment tool designed to automatically detect potential network vulnerabilities using an extensive battery of penetration tests. This graphical software utility provides a repeatable and reliable method of assessing the security configuration of systems.

Internet Scanner's firewall module helps maximize a firewall's protection by allowing the user to test for dozens of known vulnerabilities and misconfigurations. Its analysis tools and graphical user interface indicate where the firewall is at risk and recommend how to control the security exposure. Internet Scanner also provides "service" scans identifying all network services enabled across the firewall.

Internet Scanner's Web server module helps harden Web servers with a suite of analytical tools that reports potential vulnerabilities and misconfigurations and suggests methods of reducing system exposure. Internet Scanner audits and tests the operating system running the Web servers, the Web server application itself, and CGI scripts in the Web applications. Security vulnerabilities in the Web site are identified in a comprehensive Hyper-Text Markup Language (HTML) report describing the vulnerabilities along with recommended corrective actions.

TITLE

Kane Security Analyst (KSA)

AUTHOR

Intrusion Detection Incorporated

SOURCE

http://www.intrusion.com/product/ksa_nt.htm

KEYWORDS

misuse detection, system monitoring, comprehensive vulnerability analysis

CONTACT INFORMATION

Daniel Dorr
Intrusion Detection, Inc.
217 E 86th St., Suite 213
New York, NY 10028
Telephone: 212.348.8900.x302
Facsimile: 212.427.9185
E-mail: info@intrusion.com
URL: http://www.intrusion.com/contact.htm

REQUIREMENTS

Windows NT. Targets Windows NT and Novell Netware.

Root privileges

AVAILABILITY

Commercially available from http://www.intrusion.com

ABSTRACT:

KSA assesses the security status of a Novell and Windows NT network and generates reports in six areas: password strength, access control, user account restrictions, system monitoring, data integrity, and data confidentiality.

The database of known vulnerabilities that KSA uses contains password cracking tests, permissions across domains, C2 security, trust relationships, event logs, insecure partitions, audit policy compliance, uninterruptible power supply (UPS) status, excessive rights, registry security settings, guest ID configuration, and NT services.

New features include an interactive registry assessment, access control list (ACL) maps, and Kane File Rights for NTFS volumes. The Kane File Rights is an interactive tool included with the KSA that allows the user to automatically audit rights and privileges associated with various users, groups, and directories. The report generated by this audit includes percentages of compliance with the settings entered by the user.

L0PHTCrack 2.0

TITLE

L0PHTCrack 2.0

AUTHOR

L0PHT Heavy Industries

SOURCE

http://www.L0pht.com/L0phtcrack/

KEYWORD

password cracker

CONTACT INFORMATION

L0pht Heavy Industries
P.O. Box 990857
Boston, MA 02199
Telephone: Unavailable
Facsimile: Unavailable
E-mail: info@L0pht.com & admin@L0pht.com
URL: http://www.L0pht.com/

REQUIREMENTS

Windows 95/NT 4.0, source code available for UNIX (command line only). Targets Windows NT 4.0.

AVAILABILITY

Shareware with a 15-day free trial period, $50 registration fee.

ABSTRACT

This is a comprehensive password cracker for Windows NT system and local area network (LAN) manager passwords. The latest version has the builtin capability to extract encoded passwords from registry SAM files as well as directly from the system registry. Once passwords have been extracted, they are subject to a configurable brute force password attack.

NETECTIVE

TITLE

Netective

AUTHOR

NETECT Inc.

SOURCE

http://www.netect.com/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

NETECT Inc.
212 Northern Avenue
West 1, Suite 300
Boston, MA 02210
Telephone: 617.753.7370
Facsimile: 617.753.7350
E-mail: sales@netect.com
URL: http://www.netect.com

REQUIREMENTS

SunOS 4.14, Solaris 2.5.1, HP UX 10.x, Windows NT. 50 MB free hard disk space, 64 MB minimum RAM, access to a local CD-ROM drive. JAVA-compatible UNIX, HTML browser, GUI (graphical user interface) for UNIX (e.g., X-Windows, Motif), root privileges.

AVAILABILITY

Commercially available from http://www.netect.com/

ABSTRACT

Netective identifies security vulnerabilities at both the operating system level and the network level. Netective validates the system using MD5 checksums and other security checks on system files, operating system patches, file permissions, and system passwords. Netective includes a dictionary-based password cracker.

Netective modules include the following:

The Network Module maps all ports to detect potential weak points. Each detected port is subjected to appropriate hacking attempts by the port checker. Special care is given to specific services such as NFS and RPC.

The Operating System Module checks system files, patches, MD5 checksums, permissions, and passwords across the system.

The Database Module contains a library of security vulnerabilities and their respective fixes and/or patches. It is updated regularly by NETECT.

A Graphical User Interface Module displays system status and analysis. Detected breaches and their recommended corrective actions are all presented in rich hypertext.

TITLE

NetRecon

AUTHOR

AXENT Technologies, Inc.

SOURCE

http://www.axent.com/netrecon/html/orderform.htm

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

AXENT Technologies, Inc.
2400 Research Boulevard
Rockville, MD 20850
Telephone: 301.258.5043
Facsimile: 301.330.5756
E-mail: sundav@axent.com
URL: http://www.axent.com/

REQUIREMENTS

Operates on Windows NT. Targets UNIX and Windows NT servers, NetWare networks, Windows workstations, mid-range systems, mainframes, routers, gateways, Web servers, firewalls, name servers, and others.

AVAILABILITY

Commercially available from http://www.axent.com/netrecon/html/orderform.htm and priced at $1,995 for limited scan of a single class C network or $9,995 for a license to scan an unlimited number of networks. Demo available from http://www.axent.com/netrecon/surveyde.htm.

ABSTRACT

OmniGuard/NetRecon runs on a Windows NT workstation and probes networks and network resources. NetRecon performs internal and external scans of the network. UltraScan exploits multiple protocols and methods to detect vulnerable network resources. NetRecon executes parallel scans of the network systems, devices, servers, firewalls, etc., for common vulnerabilities. NetRecon's probes are organized into a hierarchy. For example, one process looks for password information from an NIS server, another process tries to crack passwords, while a third looks for servers with rlogin (remote login) services to see whether the cracked user passwords will provide access.

A few of the vulnerabilities that NetRecon checks for include resources discovered, exec service enabled, smtp decode alias enabled, null session access obtained, user level access obtained, discovered system type, nis encrypted password obtained, password cracked using small/large dictionary, local disks mountable via smb, NetWare notification password trap possible, and port [number] active.

TITLE

NetSonar

AUTHOR

WheelGroup Corporation
Acquired by Cisco Systems on 3/12/98

SOURCE

http://www.wheelgroup.com/netsonar/sonar.html

KEYWORD

comprehensive vulnerability analysis

CONTACT INFORMATION

Joel McSarland
WheelGroup Corporation
13750 San Pedro, Suite 670
San Antonio, TX 78232
Telephone: 210.494.3383
Facsimile: 210.494.6303
E-mail: info@wheelgroup.com
URL: http://www.wheelgroup.com/contact/1contact.html

REQUIREMENTS

Solaris 2.5x or 2.6. Hardware: 32 MB RAM, 2 GB hard drive, TCP/IP network interface, CD-ROM drive, HTML browser

AVAILABILITY

Commercially available with an entry class "C" license starting at $2,995.

ABSTRACT

NetSonar is a vulnerability scanner and network mapping system. Using NetSonar from a central console, the user can assess the security state of an enterprise's entire network, track historical vulnerability trends, and create reports of potential security risks.

Launched from an intuitive graphical user interface at a central console, NetSonar runs in either manual or automatic mode. It can also run specialized profiles to look for certain sets of vulnerabilities, which enables the user to quickly determine whether the vulnerabilities previously detected still exist.

NetSonar can scan a large number of range of unspecified Internet Protocol (IP) addresses. NetSonar can comprehensively scan all systems on a network, including all firewalls, web servers, routers, switches, and other systems. NetSonar Entry provides all of the same capabilities as NetSonar but allows for unlimited scanning of only one specific class C network address range (up to 254 computer systems) assigned by the user during installation.

To protect against potential misuse of the product, all NetSonar scans are identified by an "electronic fingerprint" tied to the authorized, licensed user.

NOTE: On March 12, 1998, Cisco Systems completed its acquisition of WheelGroup Corporation.

TITLE

Network Security Scanner (NSS)

AUTHOR

Douglas O'Neal

SOURCE

ftp://jhunix.hcf.jhu.edu/pub/nss/README

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Douglas O'Neal
The Johns Hopkins University
3400 North Charles Street
Baltimore, MD 21218
Telephone: 410.516.8000
Facsimile: n/a
E-mail: Doug.ONeal@jhu.edu
URL: http://www.jhu.edu/

REQUIREMENTS

UNIX (Perl script), ftplib.pl

AVAILABILITY

Freely available from ftp://jhunix.hcf.jhu.edu/pub/nss

ABSTRACT

Network Security Scanner (NSS) scans individual remote hosts and entire subnets of hosts for various simple network security problems. The majority of the tests can be performed by any nonprivileged user on a typical UNIX machine. The only test currently implemented that requires root privileges is the check for a insecure hosts.equiv file. This test requires that a fake username (e.g., bin) be fed into rexec.

NSS will not create any files on remote machines nor will it run any nontrivial programs on remote machines.

The only nonstandard external program it invokes is ypx, a program that attempts to download the password map from a NIS server. Ypx was posted in comp.sources.misc and is archived in volume 40. NSS also requires the ftplib.pl package if running Perl version 4.x. Ftplib.pl is available from several Perl archives, for example ftp://anubis.ac.hmc.edu/pub/perl/library/ftplib.pl.gz

This program was developed on a DECstation 5000 running Ultrix 4.4. It has had superficial portability checks made under SunOS 4.1.3 and Irix 5.2, but extensive work has not been performed from those platforms.

TITLE

Nfsbug

AUTHOR

Leendert van Doorn

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/nfsbug/

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Leendert van Doorn
Department of Mathematics and
Computer Science
Vrije Universiteit
De Boelelaan 1081A
1081 HV Amsterdam, THE NETHERLANDS
Telephone: 31.20.444.7762
Facsimile: 31.20.444.7653
E-mail: leendert@cs.vu.nl
URL: http://www.asmodeus.com/
archive/Xnix/nfsbug/nfsbug.c

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu /pub/tools/unix/nfsbug/

ABSTRACT

Nfsbug checks for a variety of configuration errors in NFS, mountd, and portmapper daemons. Tests check for specific NFS problems and bugs such as finding worldwide-exportable file systems, determining whether the export list really works, determining whether file systems are mountable through the portmapper, guessing file handles, exploiting the mknod bug, and the uid masking exploit.

OMNIGUARD/ESM

TITLE

OmniGuard/ESM

AUTHOR

AXENT

SOURCE

http://www.axent.com/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

AXENT Technologies, Inc.
2400 Research Boulevard
Rockville, MD 20850
Telephone: 301.258.5043
Facsimile: 301.330.5756
E-mail: info@axent.com
URL: http://www.axent.com/support/support.htm

REQUIREMENTS

Extensive software platform support for manager and agent components: Windows NT, NetWare, VMS, IBM-AIX, HP-UX, SunOS, IRIX, and others.

AVAILABILITY

Commercially available from http://www.axent.com/product/esm/esm.htm

ABSTRACT:

Omniguard/Enterprise Security Manager (ESM) is a platform-independent security management tool that enables the user to manage and evaluate diverse systems according to unique, customizable security policies. It also has an application Programming interface (API) that can be used to customize and integrate security management for other security products, applications, and databases.

The ESM architecture has three components: the graphical user interface (GUI), manager, and agent. These three components are supported on multiple software platforms, although the GUI is limited to UNIX systems compatible with X-Windows, Windows 3.x, 95, and NT. Agents contain executable modules that perform security checking and correction (based on policies) at the server, workstation, database, or application level. Agents can be run manually or on an automated schedule. The manager and GUI serve as interfaces that manipulate agents. Managers can also be used to set and apply security policies such as account integrity, back-up integrity, file access violations, file attributes, virus checking, proper login parameters, trivial passwords, system auditing, and e-mail holes.

Reports can be generated from these results that show the percentage of network resources complying with a pre-determined policy.

TITLE

Perl Cops

AUTHOR

Dan Farmer

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/cops-perl.tar.gz

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107
Telephone: 626.296.2400
Facsimile: 626.296.4130
E-mail: security@earthlink.net
URL: http://www.earthlink.net/company/farmer.html

REQUIREMENTS

UNIX (Perl script)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/cops-perl.tar.gz

ABSTRACT

Perl Cops is a security toolkit that examines a system for a number of known weaknesses and alerts the system administrator to them. This is a smaller, Perl version of Computer Oracle and Password System (COPS).

The user can specify the target (uid or gid) on the command line, using the -l option to generate PAT for a goal, and use -f to preload file owner, group and mode information. This preloading is helpful in terms of speed and avoiding file system "shadows." Features include caches for the passwd/group file entries for faster lookups.

PINGWARE

TITLE

PINGWARE

AUTHOR

Bellcore

SOURCE

http://www.bellcore.com

KEYWORD

comprehensive vulnerability analysis

CONTACT INFORMATION

Bellcore
8 Corporate Place, PYA 3A-184
Piscataway, NJ 08854-4156
Telephone: 800.521.2673
Facsimile: 732.366.2559
Email: telecom-info@bellcore.com
URL: http://telecom-info.bellcore.com/

REQUIREMENTS

SunOS 4.1 or above, Solaris 2.3, HP-UX 9.x

AVAILABILITY

Commercially available from http://telecom-info.bellcore.com/. Refer to document number OOA-1005

ABSTRACT

PINGWARE systematically scans and tests all the systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) based network from a single workstation. It checks for security vulnerabilities on the target system from the network (i.e., outside the system). It simulates an intruder by exploiting common configuration errors and known bugs in TCP/IP-based services to access the system from the network. It identifies the systems vulnerable to attack and generates a report detailing the weak points in the network.

Features include multiprocessing testing capability, network inventory, retrieval of key system files, reporting and results management. Vulnerability tests include finger, ftp, http, NFS, rlogin/rsh, rpcinfo, sendmail, tftp, xhost, and password cracking.

RISKWATCH 7.1

TITLE

RiskWatch 7.1 for Information Systems

AUTHOR

RiskWatch

SOURCE

http://www.riskguard.com/prod01.htm

KEYWORDS

risk analysis

CONTACT INFORMATION

Caroline R. Hamilton
900 Bestgate Rd., Suite 210
Annapolis, MD 21401
Telephone: 410.224.4773
Facsimile: 410.224.4995
E-mail: riskwatch@riskguard.com
URL: http://www.riskguard.com/prod01.htm

REQUIREMENTS

Windows 3.1x, Windows for Workgroups, Windows 95, Windows NT 3.51 and 4.0

AVAILABILITY

Commercially available from http://www.riskguard.com/

ABSTRACT

RiskWatch 7.1 for Information Systems conducts automated risk analysis and vulnerability assessments of information systems, including data centers, application programs, facilities, networks, and field offices. RiskWatch uses data generated by the risk analysis to provide on-line risk management and generate a variety of reports. RiskWatch is completely customizable by the user, including allowing the user to create new asset categories, threat categories, vulnerability categories, safeguards, question categories, and question sets. Users can also automatically import questions and data created by other users into their analysis.

RiskWatch automatically creates questionnaire diskettes, which are used by respondents and returned to the risk analysis manager for processing. Diskettes are created by the RiskWatch software on high or low density 3.5" floppy diskettes. Executables for the diskettes are included on the diskette. Users may generate an unlimited number of questionnaire disks.

SATAN

TITLE

Security Analysis Tool for Auditing Networks (SATAN)

AUTHOR

Dan Farmer
Wietse Venema

SOURCE

http://www.fish.com/satan/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Dan Farmer
3100 New York Drive
Pasadena, CA 91107
Telephone: 626.296.2400
Facsimile: 626.296.4130
E-mail: security@earthlink.net
URL: http://www.earthlink.net/company/farmer.html

REQUIREMENTS

UNIX (Perl script, expect, C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/satan/

ABSTRACT

SATAN scans systems connected to the network noting the existence of well-known, often-exploited vulnerabilities. SATAN examines a remote host or set of hosts and gathers as much information as possible by remotely probing NIS, finger, NFS, ftp and tftp, rexd, and other services. This information includes the presence of various network information services as well as potential security flaws involving misconfigured setup and network services and known bugs in system or network utilities. It then can either report on these data or use an expert system to further investigate any potential security problems. SATAN consists of several sub-programs, each of which is an executable file that tests a host for a given potential weakness. Additional test programs can be used by including the executable in the main directory with the extension ".sat." The driver generates a set of targets (using DNS and a fast version of ping together to get "live" targets) and then executes each of the programs on each of the targets. Three depths of scans are offered: light, normal, and heavy. A data filtering/interpreting program analyzes the output and a reporting program produces formatted output.

SATAN has not been updated since its development (c. 1995) and may not be able to detect certain vulnerabilities. For additional information, see: CIAC Notes 95-07 & CIAC Notes 95-08.

TITLE

Secure Sun

AUTHOR

David Safford

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/secure-sun-check

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

David Safford
Director, TAMU Supercomputer Center
Texas A&M University
College Station, TX 77843-0100
Telephone: 409.845.1004
Facsimile: 409.845.0727
Email: d-safford@tamu.edu
URL: http://www.cs.tamu.edu/

REQUIREMENTS

UNIX (shell script). Specific to SunOS 4.0.3 and 4.1.

No special privileges.

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/secure-sun-check

ABSTRACT

This program checks for 14 common SunOS configuration security vulnerabilities. Each test reports its findings and offers to fix any discovered problems. The program must be run as root to fix any of the problems, but it can be run from any account by replying \'n\' to any fix requests. It has only been tested under SunOS 4.0.3 on Sun4, Sun3, and Sun386i machines.

The 14 checks made are: fix ttytab to disable b -s problem, check /etc/hosts.equiv either null or at least no +, disable tftp \(nonserver\), or add secure switch \(server\), fix rcp hole, check root\'s path for, check dirs in root\'s path not writeable by others, check that /etc/passwd on ypserver does not have client line, check that uucp decode alias is removed from /etc/aliases, check /etc/utmp is not world writeable, check that rexd is disabled in /etc/inetd.conf, disable login shell for uucp, check for null /.rhosts, check for accounts with no password, and check for back-door root accounts.

SNOOPY TOOLS

TITLE

Snoopy Tools

AUTHOR

The MITRE Corporation

SOURCE

http://infosec.nosc.mil/content.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

W. Reid Gerhart
The MITRE Corporation, MS: B325
202 Burlington Rd
Bedford, MA 01730-1420
Telephone: 617.271.3738
Facsimile: 617.271.3957
Email: wrg@mitre.org
URL: http://www.mitre.org/resources/centers/infosec/infosec.html

REQUIREMENTS

Operate on a host (with a network interface) running UNIX (C source code). Tested on SunOS 4.x. Graphical interface to Snoopy Tools, xsnoopy, runs under the X11 window system. Requires the Motif libraries and 10 MB of disk space to compile.

AVAILABILITY

Developed for NAVCOMSTAR Vulnerability Assessment, Department of the Navy Space and Naval Warfare Systems Command Naval Information Systems Security Office, PMW 161, Prepared by Michelle Gosselin, Dan Vukelich, Len LaPadula (Ed.), The MITRE Corporation. March 1996.

ABSTRACT

Snoopy Tools is a suite of programs that determine what network services are running under Transmission Control Protocol/Internet Protocol (TCP/IP) and attempt to exploit bugs in those services. Snoopy probes hosts across a network in a non-intrusive manner by acting as an unprivileged client of the various services that are probed. The only indications that Snoopy is running are a possible brief spike in network activity and the audit log entries maintained by the hosts' servers.

Snoopy remotely probes hosts to determine whether selected security flaws are present in TCP/IP network services. It can act as a network sniffer to capture Novell network passwords and can scan AppleTalk networks for any readable files.

When Snoopy finds a host running TFTP, it attempts to retrieve the password file for later use in a cracking attack. However, if the password file is "shadowed," meaning that the passwords were not contained in /etc/passwd but rather in a shadow password file, the opportunity to crack the passwords of valid system users is minimized.

SPI-NET

TITLE

SPI-NET

AUTHOR

Sandy Spark

SOURCE

http://ciac.llnl.gov/cstc/spi/spinet.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Sandy Spark
Computer Incident Advisory Capability
University of California
Lawrence Livermore National Laboratory
7000 East Ave.
P.O. Box 808
Livermore, CA 94550
Telephone: 510.422.8193
Facsimile: 510.423.8002
Email: ciac@llnl.gov
URL: http://ciac.llnl.gov

REQUIREMENTS

UNIX (C source). Tested on HP-UX 10.x, IRIX 5.x, SunOS 4.x, and SunOS 5.x

AVAILABILITY

Free SPI-NET distributions are limited to U.S. Government agencies and to contractors to the U.S. Department of Energy and U.S. Department of Defense. Ongoing commercialization efforts preclude free distribution and use by private industry.

ABSTRACT

SPI-NET supports multihost system security inspections managed from a designated "command host." These inspections include access control testing, system file authentication, file system change detection, password testing, and common system vulnerability checks. SPI-NET supports flexible inspection specification and scheduling, and provides reasonable default settings. All SPI-NET command and data traffic is protected by public key encryption techniques.

The binary distributions come in two forms: The "Stand-Alone" binaries support the command-host installation and are required for at least one host in a SPI-NET security domain. The "Detached" binaries provide the capability to inspect additional remote host machines under the control of the command-host. Both Stand-Alone and Detached packages come with Installation/Setup scripts for ease of installation.

STROBE

TITLE

Strobe

AUTHOR

Julian Assange

SOURCE

ftp://suburbia.net:/pub/strobe.tgz

KEYWORDS

strobe vulnerability analysis

CONTACT INFORMATION

Julian Assange
PO Box 2031 Barker VIC 3122
AUSTRALIA
Telephone: n/a
Facsimile: 61.3.9819.9066
Email: strobe@suburbia.net
proff@suburbia.net
URL: ftp://coast.cs.purdue.edu/pub/tools/unix/strobe/

REQUIREMENTS

UNIX (C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/pub/tools/unix/strobe/strobe.tgz

ABSTRACT

Strobe is a network security tool that locates and describes all listening tcp ports on a (remote) host or on many hosts. Strobe approximates a parallel finite state machine internally. In nonlinear multihost mode, it attempts to apportion bandwidth and sockets among the hosts very efficiently. On a machine with a reasonable number of sockets, Strobe can port scan entire Internet sub-domains.

System Security Scanner

TITLE

System Security Scanner

AUTHOR

Internet Security Systems

SOURCE

http://www.iss.net/prod/isb.html

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Patrick Taylor
41 Perimeter Center East
Suite 660
Atlanta, GA 30346
Telephone: 770.395.0150
Facsimile: 770.395.1972
Email: info@iss.net
URL: http://www.iss.net

REQUIREMENTS

SunoS 4.1.3-4.1.4, Solaris 2.3-2.5.1, AIX 3.2.5-4.2, HP-UX 9.05-10.x, Irix 6.2-6.4, and Linux 1.2.13+.

AVAILABILITY

Commercial. $495 for a single server license or $3,500 for a 10-server license. Evaluation copy available from company at http://www.iss.net.

ABSTRACT

System Security Scanner assesses operating system configuration, file permissions and ownership, network services, account setups, program authenticity, and common user-related security issues such as guessable passwords.

System Security Scanner is part of the SAFEsuite line of adaptive security management solutions. These technologies give a thorough view of security threats and vulnerabilities in network traffic, Web sites, firewalls, and UNIX and Windows NT operating systems. Once vulnerabilities are identified, System Security Scanner prioritizes its findings by high, medium, or low levels of risk. It provides reports and appropriate corrective actions and generates scripts to automatically correct vulnerabilities.

System Security Scanner's open database structure and highly flexible report engine provide data in both management and implementation formats.

TITLE

Tiger

AUTHOR

Doug Schales

SOURCE

ftp://coast.cs.purdue.edu/pub/tools/unix/tiger/

KEYWORDS

comprehensive vulnerability analysis

CONTACT INFORMATION

Doug Schales
Department of Computer Science
Texas A&M University
College Station, TX 77843-3112
Telephone: 409.845.5098
Facsimile: 409.847.8578
Email: Doug.Schales@net.tamu.edu
URL: http://www.cs.tamu.edu/

REQUIREMENTS

UNIX (Bourne shell script, C source code)

AVAILABILITY

Freely available from ftp://coast.cs.purdue.edu/ pub/tools/unix/tiger/

ABSTRACT

Tiger is used to check for security problems on a UNIX system. It scans system configuration files, file systems, and user configuration files for possible security problems and reports them. Tiger was originally developed to provide a check of UNIX systems on the Texas A&M campus that users wanted to access from off campus. (Clearance was provided through the packet filter.)

TITLE

ToneLoc

AUTHOR

Minor Threat and Mucho Maas

SOURCE

ftp.paranoia.com/pub/toneloc/tl110.zip

KEYWORD

war dialers

CONTACT INFORMATION

Name: Unavailable
Address: Unavailable
Telephone: Unavailable
Facsimile: Unavailable
Email: mthreat@paranoia.com -or- mthreat@ccwf.cc.utexas.edu
URL: http://oberon.ark.com/~john/frozenhell/files.html

REQUIREMENTS

Windows 3.x/95/NT, DOS 6.x, modem

AVAILABILITY

Freely available from ftp://ftp.paranoia.com/pub/toneloc/tl110.zip

ABSTRACT:

This software is designed to scan a block of telephone numbers for an active dial-up service. This tool may be useful to administrators who are unsure whether possible back doors are present in their computer or telephone network.

TRIDENT INFORMATION PROTECTION TOOLBOX

TITLE

Trident Information Protection Toolbox

AUTHOR

Trident Data Systems

SOURCE

http://www.tds.com/tb/index.html

KEYWORDS

risk analysis

CONTACT INFORMATION

Brian Finan
10455 White Granite Drive, Suite 400
Oakton, VA 22124
Telephone: 703.383.3686
Facsimile: 703.383.3530
Email: Brian_Finan@tds.com
URL: http://www.tds.com/tb/index.html#anal

REQUIREMENTS

Operates on Windows 95 and NT 4.0

AVAILABILITY

Commercially available from http://www.tds.com/tb/index.html#anal

ABSTRACT

Trident's Toolbox is a set of three complementary tools that assist in protecting critical information assets. Toolbox is a more specific and advanced version of the company's highly successful NetRISK product.

The Trident Information Protection Toolbox includes: Trident Information Protection Analyst, a comprehensive risk management software for networks; Trident Information Protection Architect, an automated network mapping and security design; and Trident Information Protection Library, a comprehensive information security database.

Analyst automates the risk assessment process, provides summary and detailed reports of the security risks present in networks, and offers solutions for reducing those risks. The Architect automatically identifies and graphically maps all of the hardware, services, and dial-up modem entry points. Library is a comprehensive reference of current computer security information. Its relational database format allows access to Analyst and Architect. The Library contains an extensive inventory of computer vulnerabilities with appropriate safeguards or patches for each vulnerability.

VISART

TITLE

Value of Information Structured Analysis of Risk Tool (VISART)

AUTHOR

Dr. Donald R. Peeples

SOURCE

National Security Agency

KEYWORDS

risk analysis

CONTACT INFORMATION

Dr. Donald R. Peeples
National Security Agency (VI)
Ft. Meade, MD 20755-6755
Telephone: 410.859.4704
Facsimile: n/a
Email: n/a
URL: http://www.nsa.gov/

REQUIREMENTS

Tool is currently under development.

AVAILABILITY

Tool is currently under development

ABSTRACT

VISART is a risk management tool currently under development by Dr. Donald Peeples at NSA's Information Security systems Office (ISSO). This tool allows the user to analyze systems, their vulnerabilities, and possible threats, and quantify what types of countermeasures are justifiable in terms of cost. The process begins with the collection of data to describe baseline procedures (risks and probabilities), including total aggregated risk. Once this is completed, a set of appropriate countermeasures are suggested, and the tool can be rerun to determine actual effectiveness. (Cost is based on level of security.)

TITLE

XScan

AUTHOR

Unknown

SOURCE

http://www.giga.or.at/pub/hacker/unix

KEYWORDS

simple vulnerability analysis

CONTACT INFORMATION

Name: Unavailable
Address: Unavailable
Telephone: Unavailable
Facsimile: Unavailable
Email: pendleto@math.ukans.edu
URL: Unavailable

REQUIREMENTS

Linux or SunoS, 4.1.4, X system (C source code)

AVAILABILITY

Freely available from http://www.giga.or.at/pub/hacker/unix/xscan.tar.gz

ABSTRACT

This utility scans a host, or a range of hosts, for unprotected X displays. If an unprotected display is discovered, this utility monitors that connection and logs all keystrokes made on the display. This is a useful tool to exploit passwords that may be obtained from the local machine or remote machine depending on what the scanned target is doing with the open display. System administrators can use this tool to determine whether users are adequately restricting those hosts that can connect to their active X sessions.

Information Assurance Technology Analysis Center

Information Assurance Tools Report **Spring 98**

DISTRIBUTION STATEMENT A – Approved for public release, distribution is unlimited

VULNERABILITY ANALYSIS